PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-160829
(43)Date of publication of application : 25.06.1993

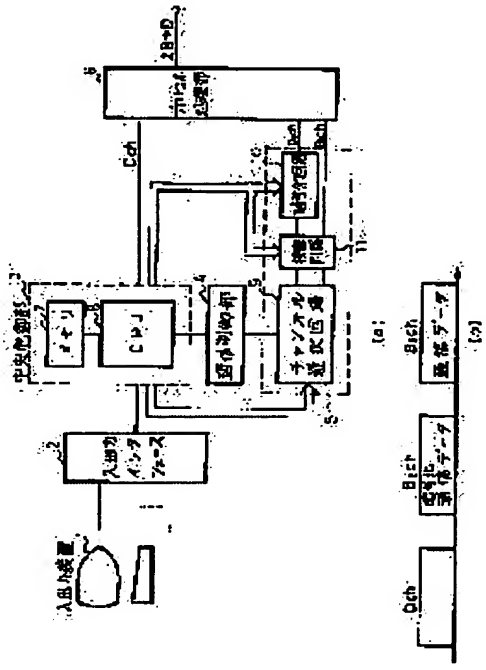
(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00
H04L 1/22
H04L 29/04
H04M 11/00

(21)Application number : 03-322122
(22)Date of filing : 05.12.1991

(71)Applicant : NEC CORP
(72)Inventor : FUJII KATSUYUKI

(54) ISDN COMMUNICATION EQUIPMENT

(57)Abstract:
PURPOSE: To attain data communication by sending communication data of the same content through the use of two B channels, allowing a reception terminal equipment to cipher a plain text and to compare the result with the communication data while the communication data are verified by both a caller side and a receiver side.
CONSTITUTION: When a caller subscriber 21 outputs an important data communication request to a caller terminal equipment 22, the terminal equipment 22 generates a ciphering key use random number γ as a call for using two communication channels and sends a setup message SETUP. A caller exchange 24 sends a similar setup message IAM. A called exchange 25 connects similarly the two communication channels to a called terminal equipment 27 to send a message SETUP. The terminal equipment 27 sends a reply message CNNECT together with the random number γ received by the SETUP based on a communication enable notice from a subscriber 28, sends a ciphering key to a ciphering circuit 10, which is started, data of the communication channel are ciphered and compared with other data by a verification circuit 11, and then the communication attended with data verification is started.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－160829

(43)公開日　平成５年(1993)６月25日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/06						
	9/14						
Ｇ０９Ｃ	1/00		9194－5L				
			7117－5K	Ｈ０４Ｌ	9/ 02	Ｚ	
			8020－5K		13/ 00	３０３　Ｚ	

審査請求　未請求　請求項の数３(全　６　頁)　最終頁に続く

(21)出願番号　特願平3－322122

(22)出願日　平成３年(1991)12月５日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　藤井　克之
東京都港区芝五丁目７番１号　日本電気株式会社内

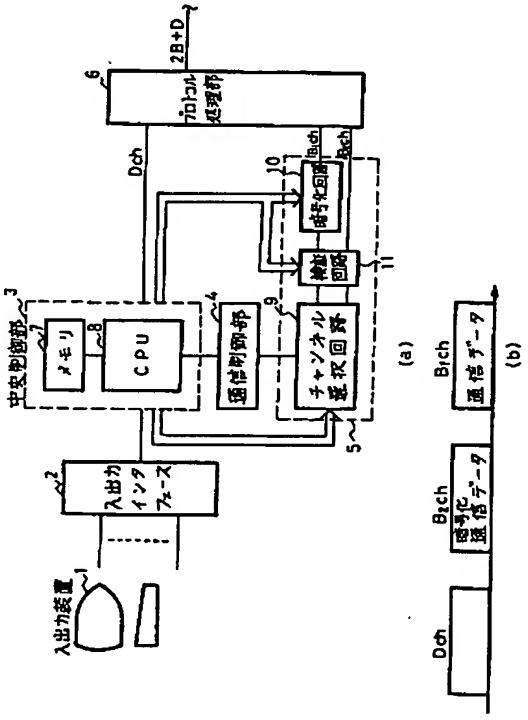
(74)代理人　弁理士　井出　直孝

(54)【発明の名称】　ＩＳＤＮ通信装置

(57)【要約】

【目的】　ＩＳＤＮによるデータ通信において、通信速度を低化させず入出力装置の種類を問わずに通信回線を検証しながら重要なデータの送受信を行う。

【構成】　ＩＳＤＮの二つのＢチャンネルを同時に使用し、同じ内容の通信データをその二つのＢチャンネルで送信するが、そのどちらか片方を暗号化して送信する。受信側ではあらかじめ受け取っている暗号化鍵により暗号化されていないデータを受信側で暗号化して、二つのＢチャンネルにより受信した通信データを比較検証することにより、データの誤りを発見する。



【特許請求の範囲】

【請求項１】　ＩＳＤＮ通信を行うための入出力装置と、この入出力装置を接続する入出力インタフェースと、この入出力インタフェースに接続されＩＳＤＮの各チャンネルおよび装置各部を制御する中央制御部と、この中央制御部に接続されＢチャンネルの通信を制御する通信制御部と、この通信制御部に二つのＢチャンネルを前記中央制御部の指示により選択して接続するチャンネル選択部と、ＢチャンネルおよびＤチャンネルのプロトコルを処理するプロトコル処理部とを備えたＩＳＤＮ通信装置において、

前記中央制御部は、

前記Ｂチャンネルに送出する信号を暗号化する暗号化鍵を発生する手段と、

前記Ｂチャンネルから受信した暗号化鍵を格納するメモリ手段とを備え、

前記チャンネル選択部は、

送受信する二つのＢチャンネル信号の片方を暗号化する手段と、

受信した片方のあらかじめ暗号化されたＢチャンネル信号および前記暗号化する手段により受信した後に暗号化されたもう片方のＢチャンネル信号を比較検証する手段とを含むことを特徴とするＩＳＤＮ通信装置。

【請求項２】　前記中央制御部には、

セットアップ信号の中に相手端末に対して検証モードであることを通知する手段を含む請求項１記載のＩＳＤＮ通信装置。

【請求項３】　前記暗号化鍵を発生する手段は、乱数の発生手段による請求項１記載のＩＳＤＮ通信装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はＩＳＤＮ通信回線の検証に利用する。特に、二つのＢチャンネルの同時接続呼の暗号化通信による通信データ検証方式に関する。

【０００２】

【従来の技術】従来例を図３を参照して説明する。図３は従来例装置のブロック図および通信信号形態を示す図である。

【０００３】周知のとおりＩＳＤＮには一つのＤチャンネルと二つのＢチャンネルがあり、通信データは通常二つのＢチャンネルにより送受信される。装置の構成は図３（ａ）に示すとおりである。

【０００４】回線の状態を検証するときには図３（ｂ）に示すように入出力装置１により、通信データをあるブロックに区切り、そのブロック単位で算出されたパリティビットなどのデータ検証用符号を通信データの前後に付加して送信し、着信側ではブロックごとに算出した符号値とデータ検証用符号を比較して、データ誤りの有無により回線状況を検証している。

【０００５】

【発明が解決しようとする課題】この従来の通信回線検証方式では、同一チャンネル上で通信データと検証用データとを送信するため、データの長さは長くなり通信データ自体の通信速度が低下することになる。即ち、検証用の付加データが小さいときには通信速度はそれほど低下しないが検証能力が低下してしまい、検証用付加データが大きいと通信速度が低下する。また、検証用付加データは各端末のソフトウェアで生成付加しているため、種類の異なる端末同士では通信できないという問題がある。

【０００６】本発明はこのような背景に行われたものであり、通信速度を低化させず入出力装置の種類を問わない通信回線検証手段を有するＩＳＤＮ通信装置の提供を目的とする。

【０００７】

【課題を解決するための手段】本発明はＩＳＤＮ通信を行うための入出力装置と、この入出力装置を接続する入出力インタフェースと、この入出力インタフェースに接続されＩＳＤＮの各チャンネルおよび装置各部を制御する中央制御部と、この中央制御部に接続されＢチャンネルの通信を制御する通信制御部と、この通信制御部に二つのＢチャンネル信号を前記中央制御部の指示により選択して接続するチャンネル選択部と、ＢチャンネルおよびＤチャンネルのプロトコルを処理するプロトコル処理部とを備えたＩＳＤＮ通信装置において、前記中央制御部は、前記Ｂチャンネルに送出する信号を暗号化する暗号化鍵を発生する手段と、前記Ｂチャンネルから受信した暗号化鍵を格納するメモリ手段とを備え、前記チャンネル選択部は、送受信する二つのＢチャンネル信号の片方を暗号化する手段と、受信した片方のあらかじめ暗号化されたＢチャンネル信号および前記暗号化する手段により受信した後に暗号化されたもう片方のＢチャンネル信号を比較検証する手段とを含むことを特徴とする。

【０００８】また、前記中央制御部には、セットアップ信号の中に相手端末に対して検証モードであることを通知する手段を含むことが望ましい。

【０００９】なお、前記暗号化鍵を発生する手段は、乱数の発生手段による構成とすることもできる。

【００１０】

【作用】重要な通信を行うに当たって、ＩＳＤＮ通信回線を検証するときに同じ内容の通信データを二つのＢチャンネルを使用して、片方は暗号化し、もう片方は暗号化していない通信データ（以下、平文という）として送信する。受信した端末では、あらかじめ受け取っている暗号化鍵を用いて送られてきた平文を暗号化し、あらかじめ暗号化されて送られてきた通信データと比較することにより、データ誤りを発見するというものである。

【００１１】二つのＢチャンネルで同じ内容の通信データを送受信するので、あたかも効率が低いように感じるがデータ検証用符号を通信データの前後に付加しないの

で、データの長さを最小限にできることから実際には通信回線の検証を行いながら、より効率のよいデータ通信が実現できる。

【００１２】片方を暗号化する理由としては通信回線に何らかの異常があり、ある一定の規則性により通信データが書換えられてしまうような場合、平文を同時に送信したのでは両方とも同様に書換えられるため、受信側で二つのデータを比較してもデータ誤りが発見できないからである。片方を暗号化することにより、デジタル信号の「１」および「０」の配列を変えてあるので、ある一定の規則性により通信データが書換えられたとしても、受信側で検証すれば、平文を暗号化した通信データと、もともと暗号化されて受信された通信データとではデータ内容が異なりデータ誤りを発見できる。

【００１３】

【実施例】本発明実施例装置の構成を図１を参照して説明する。図１は本発明実施例装置のブロック図および通信信号形態を示す図である。

【００１４】本発明はＩＳＤＮ通信を行うための入出力装置１と、この入出力装置１を接続する入出力インタフェース２と、この入出力インタフェース２に接続されＩＳＤＮの各チャンネルおよび装置各部を制御する中央制御部３と、この中央制御部３に接続されＢチャンネルの通信を制御する通信制御部４と、この通信制御部４に二つのＢチャンネル信号を中央制御部３の指示により選択して接続するチャンネル選択部５と、ＢチャンネルおよびＤチャンネルのプロトコルを処理するプロトコル処理部６とを備えたＩＳＤＮ通信装置において、中央制御部３は、前記Ｂチャンネルに送出する信号を暗号化する暗号化鍵を発生する手段をＣＰＵ８に備え、前記Ｂチャンネルから受信した暗号化鍵を格納するメモリ手段としてのメモリ７を備え、チャンネル選択部５は、送受信する二つのＢチャンネル信号の片方を暗号化する手段としての暗号化回路１０を含み、受信した片方のあらかじめ暗号化されたＢチャンネル信号および暗号化回路１０により受信した後に暗号化されたもう片方のＢチャンネル信号を比較検証する手段としての検証回路１１を含む構成である。

【００１５】また、中央制御部３のＣＰＵ８には、セットアップ信号の中に相手端末に対して検証モードであることを通知する手段を含む。

【００１６】また、前記暗号化鍵を発生する手段は、ＣＰＵ８における乱数の発生手段による構成である。

【００１７】本発明実施例装置による通信信号形態は図１（ｂ）に示すように、同じ内容の通信データを二つのＢチャンネルで送出するが一方は暗号化回線１０により暗号化されて送出される。

【００１８】次に、図２を参照して本発明実施例装置の動作を説明する。図２は本発明実施例装置の動作を示す図である。

【００１９】発信側加入者２１が重要データ通信を行うための要求を発信側端末２２に対して出すと、発信側端末２２は二本の通信チャンネル使用の呼として、暗号化鍵となる乱数ｒを発生し、これらのデータと共に呼設定メッセージＳＥＴＵＰを送信する。これを受信した発信側交換機２４も二本の通信チャンネルを接続して、同様の呼設定メッセージＩＡＭを送信する。着信側交換機２５は着信側端末２７に同様に二本の通信チャンネルを接続して呼設定メッセージＳＥＴＵＰを送信する。着信側端末２７は着信側加入者２８からの通信許可通知により、ＳＥＴＵＰにて受信した暗号化鍵である乱数ｒと共に応答メッセージＣＮＮＥＣＴを送信し、さらに暗号化鍵を着信側の暗号化回路１０に送って起動し、暗号化されていない通信チャンネル側のデータを暗号化して、着信側の検証回路１１で他方のデータと比較することにより、データ検証を伴う通信を開始する。応答メッセージは着信側端末２７から受けた暗号化鍵と共に着信側交換機２５および発信側交換機２４を経由して発信側端末２２に伝えられる。この暗号化鍵により発信側端末２２は鍵の一致を確認し、発信側端末２２のチャンネル選択回路９を起動し、さらに暗号化鍵と共に暗号化回路１０の起動を行う。

【００２０】以上の手順により、発信側端末２２および着信側端末２７の双方で通信データ検証を行いながらのデータ通信が可能となる。

【００２１】

【発明の効果】通信速度を低化させずしかも入出力装置の種類を問わずに通信回線の検証ができる。

【図面の簡単な説明】

【図１】本発明実施例装置のブロック図および通信信号形態を示す図。

【図２】本発明実施例装置の動作を示す図。

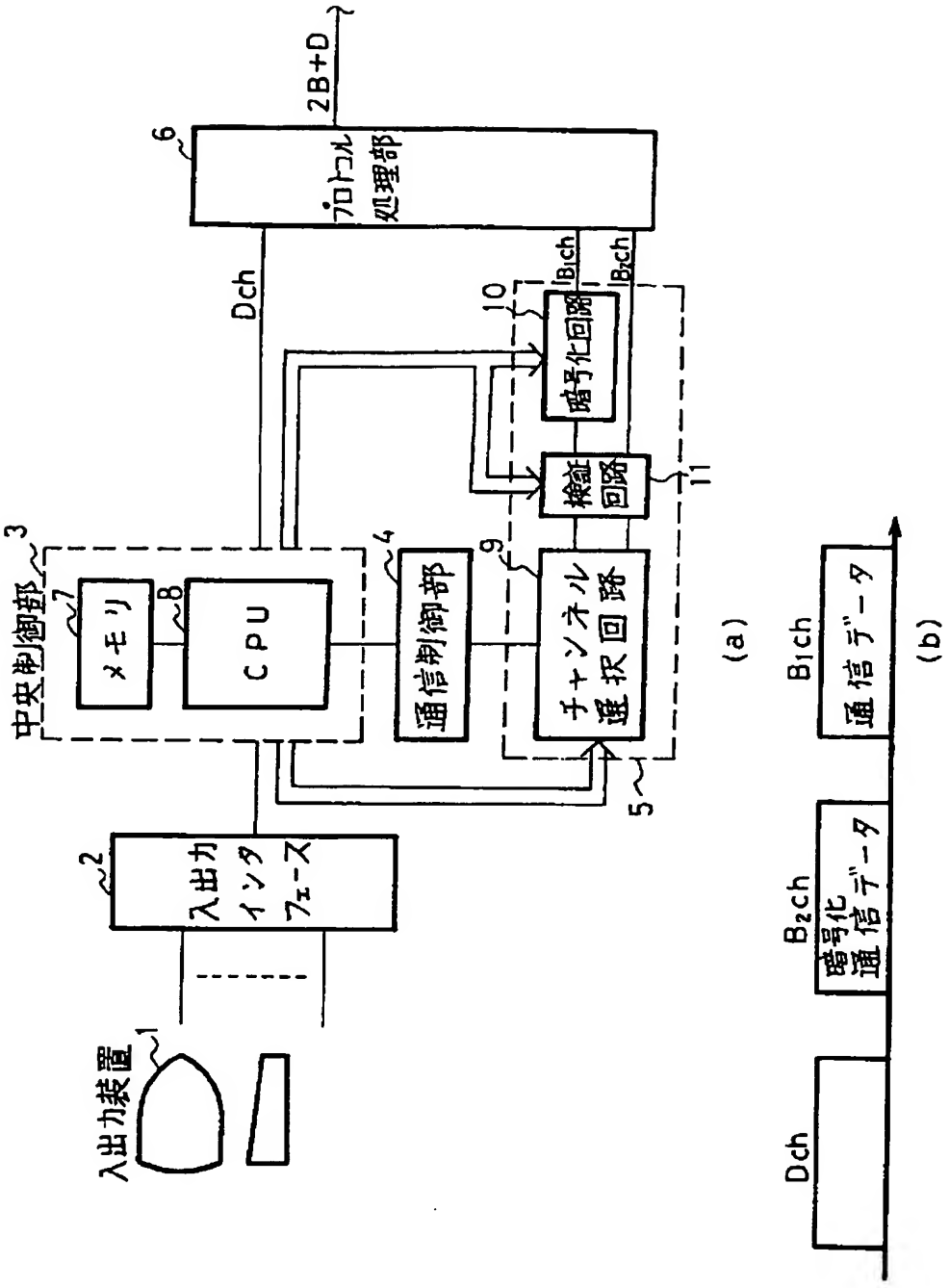
【図３】従来例装置のブロック図および通信信号形態を示す図。

【符号の説明】

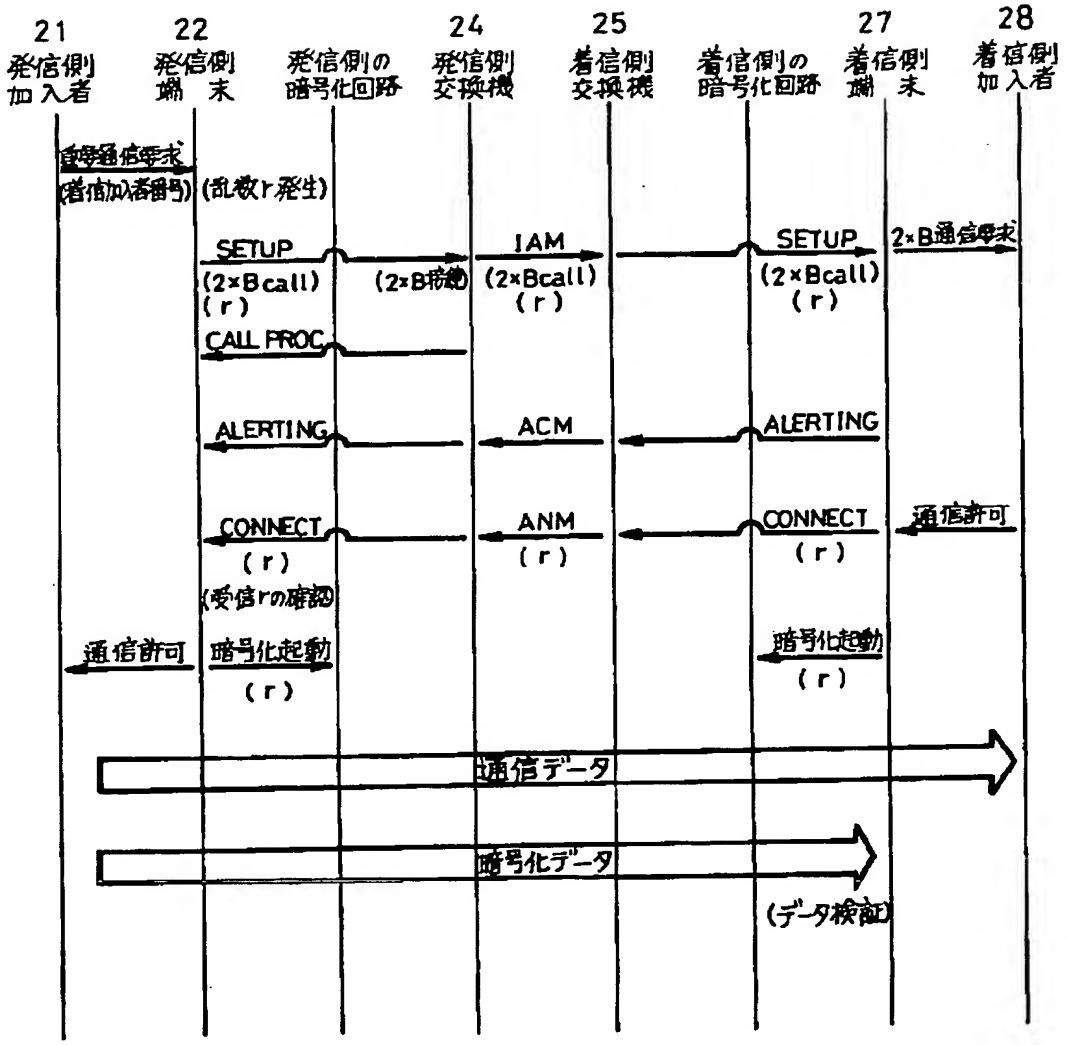
１　入出力装置
２　入出力インタフェース
３　中央制御部
４　通信制御部
５　チャンネル選択部
６　プロトコル処理部
７　メモリ
８　ＣＰＵ
９　チャンネル選択回路
１０　暗号化回路
１１　検証回路
２１　発信側加入者
２２　発信側端末
２４　発信側交換機
２５　着信側交換機

２７　着信側端末　　r　乱数
２８　着信側加入者

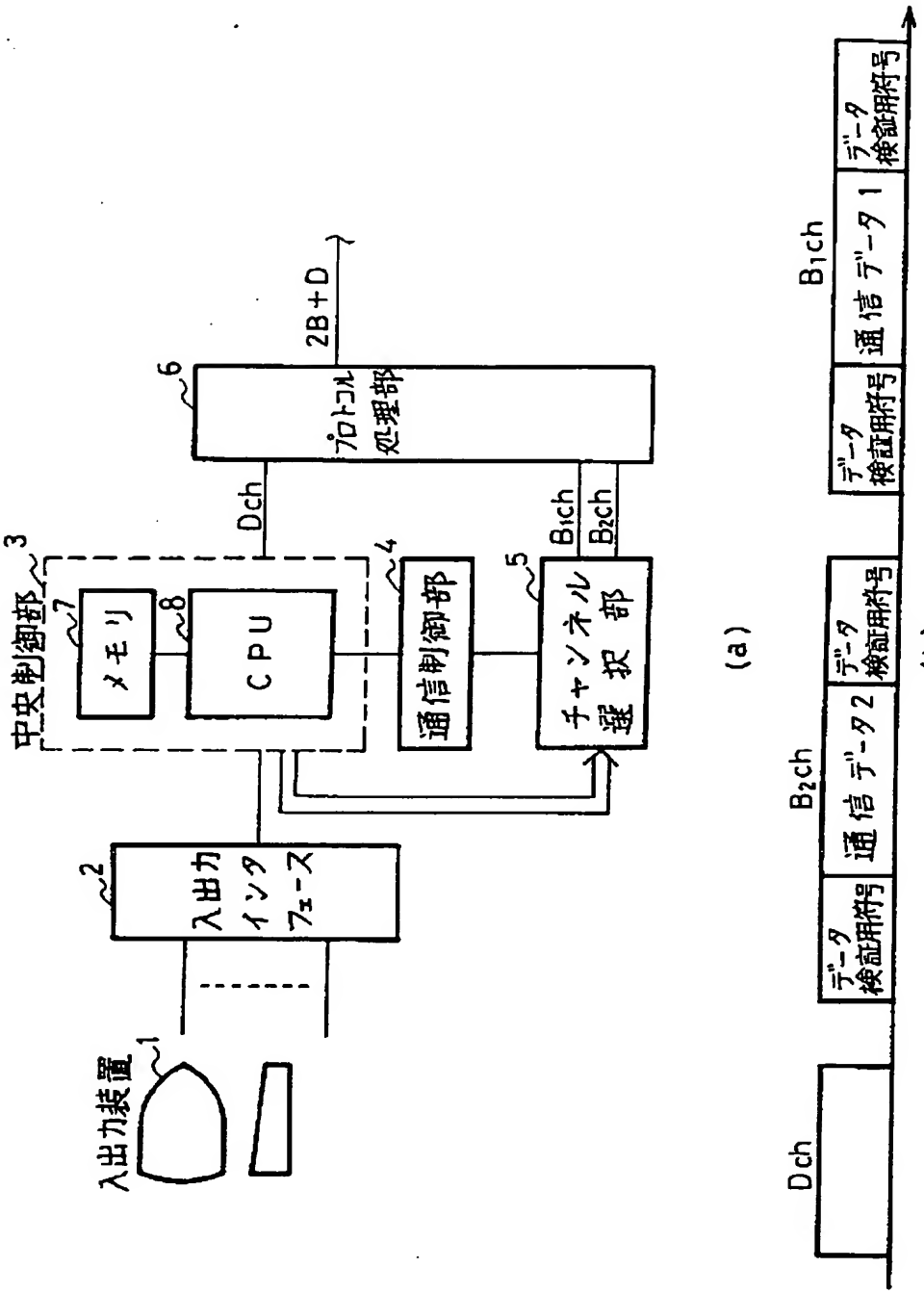
【図１】



【図２】


21
発信側加入者
22
発信側端末
発信側の暗号化回路
24
発信側交換機
25
着信側交換機
着信側の暗号化回路
27
着信側端末
28
着信側加入者
着呼通信要求
(着信加入者番号)
(乱数r発生)
SETUP
(2×Bcall)
(r)
(2×B接続)
IAM
(2×Bcall)
(r)
SETUP
(2×Bcall)
(r)
2×B通信要求
CALL PROC
ALERTING
ACM
ALERTING
CONNECT
(r)
ANM
(r)
CONNECT
(r)
通信許可
(受信rの確認)
通信許可
暗号化起動
(r)
暗号化起動
(r)
通信データ
暗号化データ
(データ検証)

【図3】



フロントページの続き

(51) Int. Cl.[5]		識別記号	庁内整理番号	F I	技術表示箇所
H04L	1/22		7190−5K		
	29/04				
H04M	11/00	303	7117−5K		